Contact Person	Information Systems	**Revision**	2.1
Document	Guide 48400.001	**Effective Date**	1/01/15
		Review Date	1/01/20

CYBER SECURITY REQUIREMENTS TRAINING

This document contains the Cyber Security requirements training for Assistant Cyber Security Managers (ACSMs) and Group Administrators (GroupAdmins).

1.0 APPROVAL RECORD

- Reviewed by: Document Control Coordinator (Amy Tehan)
- Approved by: Manager, Information Systems (Diane DenAdel)
- Approved by: Chief Operations Officer (Mark Murphy)

The official approval record for this document is maintained in the Training & Records Management Office, 151 TASF.

2.0 REVISION/REVIEW INFORMATION

The revision description for this document is available from and maintained by the author.

3.0 PURPOSE AND SCOPE

To address the federal requirements for cyber security, the Department of Energy issued Order 205.1A "Department of Energy Cyber Security Management." This order requires that Ames Laboratory create and maintain a comprehensive Cyber Security Program Plan (CSPP). The CSPP serves as the security plan for ensuring the confidentiality, integrity, and availability of Ames Laboratory data. One of the topics addressed in the CSPP is cyber security program education, training, competencies, and awareness.

The Computer Security Act of 1987, the Federal Information Security Management Act (FISMA) of 2002, and the Office of Management and Budget (OMB) Circular A-130 Appendix III require that all U.S. government personnel who use computers as part of their work activities complete training on computer security awareness. Cyber security training is mandatory for Assistant Cyber Security Managers (ACSMs) and Group Administrators (GroupAdmins).

4.0 ROLES AND RESPONSIBILITIES

4.1 Directors/Associate Directors

Directors/Associate Directors have ultimate responsibility for the success of the Laboratory's cyber security program and establishing the program's overall goals, objectives and priorities.

4.2 Cyber Security Manager (CSM)

Cyber Security Manager (CSM) is an Information Systems Office staff member who directs the Laboratory's day-to-day management of the cyber security program.

4.3 Assistant Cyber Security Manager (ACSM)

Assistant Cyber Security Managers (ACSM) are appointed by the Program Director/Office Manager within their program/office to act as the point of contact for computer security and to carry out the policy and procedures. An ACSM directs the day-to-day management of the cyber security program in his or her respective program/office. ACSMs will:

- Maintain the list of systems on the network. ACSMs and Group Administrators are provided access to the Netreg system registration tool. All IP request forms must be reviewed and signed by the ACSM.

- Act as a communication point for the distribution of computer security-related information (i.e., CIAC notices) and as a representative of their users to the IS Office. ACSMs should ensure that they can effectively communicate with the users in their area to propagate security information as efficiently as possible

- Coordinate contingency plans for their areas of responsibility.

4.4 Group Administrator (GroupAdmin)

Group Administrators manage multiple computers and direct the day-to-day management of the cyber security program within their group. They design and operate computer systems and are responsible for patch and configuration management. ACSMs are also responsible for performing these functions for systems not covered by a separate Group Administrator. Group Administrators will:

- Make sure Baseline Configuration Guides are applied on systems they administer.
- Keep informed on new vulnerabilities, patches, and updates and make sure patches and updates are applied.
- Monitor system log files for suspicious activity and report to their ACSM or the IS Office.
- Monitor user accounts and manage access controls on multi-user systems.
- Design and maintain system contingency plans and perform regular system backups.
- Respond to alerts about new vulnerabilities and assist with recognizing and responding to cyber security incidents.
- Inform users of new threats, especially urgent threats.

4.5 Privileged Users

Privileged users administer their own systems, including patch and configuration management.

4.6 Users

Users directly interact with computing systems to perform Ames Laboratory work. They are responsible for knowing and following Laboratory cyber security policies and reporting any security violations or suspicious activity to the attention of the ACSM, CSM, or other proper authority. They must also maintain their systems according to the best practices outlined in the Baseline Configuration Guides and follow the established Configuration Management process. Users will be held accountable for their actions on the network. If in violation of policy, disciplinary actions may include a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

In addition, users will:

- Verify that patches and virus scan software updates are applied weekly.
- Inform their Group Administrator or ACSM when system changes affect security, such as the addition or removal of software.
- Ensure backups are performed and a system contingency plan has been developed and approved for the system.
- Change their passwords at least every 180 days.

- Maintain accounts.

5.0 PROGRAM/POLICY/PROCEDURE INFORMATION

5.1 Ames Laboratory Cyber Environment

The Ames Laboratory cyber environment consists of two enclaves, low and moderate, encompassing the computer/networked systems and devices at the Laboratory.

- Low enclave: The low controls as defined by NIST are the minimum acceptable set of security measures to meet DOE policy. These controls include password strength, basic encryption for network traffic, general event logging on systems, and physical security such as locking screens. Systems in this enclave ONLY generate, store, process, and transmit non-moderate data.

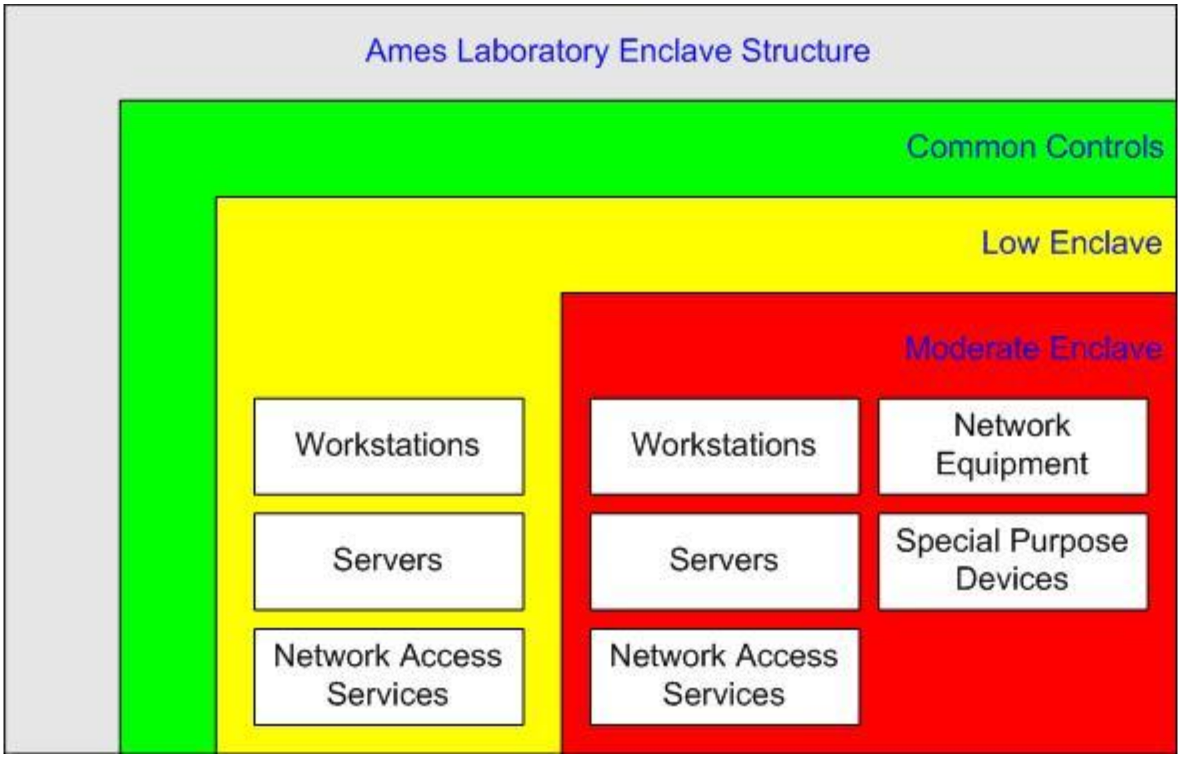
- Moderate enclave: Moderate NIST controls are additional protections designed to mitigate risks associated with sensitive, PII, patentable, and other data of elevated value to DOE. These controls specify e.g. stronger encryption requirements, the use of two-factor authentication, and increased event logging on systems. Systems in this enclave are used to generate, store, process, or transmit moderate data.

Additional information on low and moderate data is available on the Ames Laboratory website (https://www.ameslab.gov/operations/faq/what-moderate-and-low-data). Each enclave contains several virtual network segments used to isolate systems into subsets with varying exposure to cyber attacks and data sensitivity. **Only unclassified data is processed at the Laboratory.**

There are low and moderate controls for systems in each of the following categories:

- Workstations
  - Daily use systems for both administrative and scientific tasks
  - Includes desktops, laptops, smart phones, and virtual machines
- Servers
  - Systems shared by multiple users simultaneously
  - Includes central services, clusters, remote access, and internet accessible systems
- Special purpose devices
  - Devices which are tasked for specific purposes and not used for general computing
  - Includes NAS devices, instrument control systems, and printers
- Network equipment
  - Devices with the primary purpose to facilitate network communication
  - Includes host and appliance based routers, switches, firewalls, and wireless access devices
- Network access services
  - Systems used from off-site to connect to Ames Laboratory resources
  - Includes clients using VPN, wireless
  - In addition, limited use of personal equipment and sponsored visitor equipment is supported. For personal equipment, a limited baseline is established and only public internet access is provided.

Illustration of Ames Laboratory Enclave Environment



5.2 Policies and Procedures

In regard to computer usage, the Ames Laboratory has adopted the following documents to aid in conforming to Federal law, rules and regulations, and Department of Energy requirements:

- **Ames Laboratory Computing Services Policy** identifies the policies for the use and operations of information and information systems at the Laboratory. (https://wiki.internal.ameslab.gov/wiki/Cyber_Policies_and_Procedures)

- **Cyber Security Program Plan (CSPP)** implements the requirements of DOE Order 205.1 A. (https://wiki.internal.ameslab.gov/wiki/Cyber_Policies_and_Procedures)

- **Ames Laboratory Cyber Security Procedure** defines the processes employed to ensure that the policy is effectively implemented, maintained, and audited.

- **Ames Laboratory Site Risk Assessment** contains guidance on risk assessment and risk mitigation strategies. (https://wiki.internal.ameslab.gov/wiki/Cyber_Policies_and_Procedures)

- **DOE Directives, Regulations, Policies and Standards** (https://www.directives.doe.gov/) (Look at directives by number and select “Series 200 Information and Analysis” to access Cyber Security Directives, Notices and Guides.)

5.3 Acknowledgement Statements

Acknowledgement statements indicate acceptance of Ames Laboratory policies. Ames Laboratory policies that provide acknowledgement information and/or statements include:

- Rules of Behavior for low and moderate enclaves. (https://www.ameslab.gov/operations/faq/what-are-the-rules-behavior-using-the-ames-laboratory-network)
- Warning banners on all systems with interactive logins. (https://wiki.internal.ameslab.gov/wiki/Banner_Text)
- Web page privacy statements posted on Ames Laboratory web sites. (http://www.ameslab.gov/privacy)

5.4 Access Control

Account Management

Each user should be given a unique access account on systems as needed. There should be one primary Group Administrator per system.

Account Initiation

To gain access to central services, a user must complete and sign a Request for a New Account Form (form 48400.016) that indicates what services are being requested. The user's Group Administrator and ACSM verify the identity of the user and approve and sign the form.

Account Termination

After IS disables a terminated employee's central services account, the employee's ACSM or group administrator disables any standalone accounts and changes any other passwords the user may have known. The ACSM should update records to reflect and verify this change in account status. If requested, email accounts may be forwarded for up to 90 days after the employee's termination.

In addition to employment termination, user accounts must be disabled if the account is idle for 180 days or longer. Local accounts will need to be periodically tested by the ACSM or group administrator using system specific tools to determine if any accounts need to be manually disabled.

Password Use and Management

A password is an employee's key to Ames Laboratory computing resources, and good password maintenance is critical to ensuring a safe computing environment. The DOE defines certain password characteristics that must be met.

Passwords must be:

- At least 8 characters long.
- Not based on the username or a dictionary word.
- Comprised of mixed case, symbols, and digits and contain a non-numeric character in

the first and last position.

- Changed every 180 days.
- Not reused to access other internet resources (e.g., a hotmail account).
- Easy to remember but hard to guess (e.g., a phrase or acronym)
- Not shared with anyone else.

System Access

Machine Registration

New systems are registered via the IP Address Request Form (Form 48400.017). Once an IP address is assigned to the system, the ACSM must verify within one week that he or she has applied the baseline guide settings to the system. Initially system information will be set in Netreg using the form; however, the ACSM or group administrator should update any changes to system make/model, operating system, or location in Netreg. For access to Netreg and help using the system, contact the IS office.

Personally-Owned Systems

Personally-owned systems are purchased by an individual out of his or her own personal funds. These systems are not required to implement the full security baseline guides but must conform to a limited set of baselines for network access:

- Verify the following:
  - A current virus scanner is installed and up-to-date.
  - A current anti-spyware tool is installed and up-to-date (for Microsoft Windows).
  - All system patches are installed and the system has a defined (preferably automatic) process for receiving updates regularly.
  - All client software that will be used to connect to or on the Ames Laboratory network is properly configured and secured.

- Use encryption to access or store any personally identifiable information (PII) (e.g., social security number, mother's maiden name, and other non-public information that could be used to compromise an individual's identity). For more information, see the PII training (Cyber Train AL-215) or the Sensitive Systems guide (http://www.ameslab.gov/guides/guidelines-sensitive-systems).

All systems connected to the internal network are managed under the Rules of Behavior for low risk systems (https://www.ameslab.gov/operations/faq/what-are-the-rules-behavior-using-the-ames-laboratory-network). The same Rules of Behavior and responsibilities apply to both personally-owned and Laboratory-owned systems used on the network.

Visitor & Guest Access

Visitors and guests can access the Internet from Ames Laboratory. Two access methods are available:

1. Wireless network access requires a Captive Portal account; this account can be obtained from the IS office or any ACSM. Users will only be able to access the internet from this network; no access to internal Ames Laboratory resources is available. For instructions and more information see https://www.ameslab.gov/operations/is/visitor-information

2. Using an Ethernet connection, a visitor computer can be registered on the network in the visitor/conference VLAN. This VLAN allows internet access and also permits VPN connections back to the internal network. Prior to the visit, verify with IS that the network port which will be used is in the visitor / conference VLAN. The Ames Laboratory Captive Portal service is a mechanism for providing Internet access to visitors. Visitors can use Captive Portal service to access the web via wired connections in conference rooms or wireless connections where available throughout Ames Laboratory.

For more information about how a sponsor of a visitor can request a guest/visitor account, please see our FAQ: How do I register a short-term visitor to use the network (https://www.ameslab.gov/operations/faq/what-captive-portal-and-how-do-i-use-it).

Any visitors using existing computing resources must have their own unique username and password on the system. Temporary or guest accounts should not be used, even if the visitor will only be on-site for a short time.

For those visitors requiring only remote access to resources (i.e., there are no plans for an on-site visit), the system owner, group administrator, or ACSM should submit a Cyber-only Access Form (https://www.ameslab.gov/is/documents/form/cyber-only-access).

Portable Device Access
Portable devices are treated as any other computing device. If they can be assigned an IP address, they must be registered using the normal process for network access. Baseline guides are not available for portable platforms other than full laptop computing devices. To ensure that these systems are securely configured, please schedule a visit with IS staff to review device settings.

In addition, users traveling with laptops must ensure that:
Prior to travel:

- Ensure a backup of the system has been made; don’t take any information off-site that cannot be lost!
- The Off-Site Use: ADP Equipment Form is complete (Form 58301.005, available from the Purchasing and Property Services office or online at https://www.ameslab.gov/purchasing/documents/form/site-adp-equipment-authorization-form.

While the laptop is absent:

- The laptop is not left unattended, especially in public areas such as hotel lobbies, airports, and restaurants.
- The system is only on a network when network resources are required. For example, don’t be on a hotel’s wireless connection if the network is not being used.

When the laptop returns:

- A full virus scan and spyware scan are run on the system before connecting to the Ames Laboratory network again.

Sensitive System Access

Sensitive systems are systems storing moderate impact data (e.g., Work for Others, PII, medical, or proprietary information). These systems require additional controls and protections; for example, IS must manage all user accounts on these systems directly. For more information, see the PII training (Cyber Train AL-215) or the Sensitive Systems guide (https://www.ameslab.gov/is/documents/guide/guidelines-sensitive-systems).

Wireless Access

Wireless networks are not currently a substitute for wired network connections. Wireless is an augmentation to the wired network to extend general access to common and transient areas where students, faculty, and staff gather. Appropriate wireless use includes: instructional labs, library facilities,public areas, conference rooms, and research labs.

Currently, three wireless networks are available for use. Ames Laboratory employees should register wireless devices for use on the internal wireless network. Registration is performed via the new IP Request Form. The internal wireless network uses WPA2 Enterprise link encryption, and the VLAN for this traffic permits VPN access back into the internal network.

Visitors can register systems on the visitor wireless network. This network provides WEP encryption with a known key which can be obtained from the IS office. Traffic is isolated in a network segment which has access to external Ames Laboratory services and the internet, but no VPN access.

To extend wireless access to new areas, the requesting program or department must purchase the approved IS equipment. All wireless access points must be managed by IS staff.

Due to the lack of privacy of network communication over existing wireless network technology, all wireless traffic is presumed to be insecure and susceptible to unauthorized examination. Wireless network users must employ encrypted protocols when using a wireless network connection. These encrypted protocols include: Secure Sockets Layer (SSL) for web and e-mail communication, Secure Shell (Version 2) for interactive connection, and IPSEC VPNs for general access to remote networks.

Remote Access Systems

Virtual Private Network (VPN) Access

The VPN provides a secure extension of the Ames Laboratory network to user-authenticated remote computers across the unsecured internet. VPN access is obtained by requesting a VPN account via a Request for a New Account Form (Form 48400.016). The form is available on the IS internal website (https://www.ameslab.gov/is/documents/form/new-account-request) or by contacting the IS Office. Instructions for configuring VPN software are located here: https://www.ameslab.gov/operations/is/remote-access

It is important to note that while a computer is connected via VPN it is attached to the Ames Laboratory network with an Ames Laboratory IP address. This means that traffic is passing through the Ames Laboratory network and must conform to the policies for appropriate use and behavior.

Three types of VPN access are available: PPTP, IPSec with the Cisco agent, and IPSec over L2TP without an agent. The recommended method is using L2TP without a client both for ease of setup and for security.

Secure Shell (SSH) Access
Internal Ames Laboratory computer systems are available from the internet via the secure shell protocol (SSH). SSH is an encrypted interactive logon that can be used to securely communicate over an insecure network. Instructions for using the Ames Laboratory central SSH gateway are available at http://www.ameslab.gov/node/3148. A username and password must be requested via the Request for a New Account Form (Form 48400.016) prior to providing access. The form is available on the IS website (https://www.ameslab.gov/is/documents/form/new-account-request) or by contacting the IS Office.

Work-at-Home
Ames Laboratory Directors, Program Directors, and Office Managers can designate specific employees (e.g., critical job series, employees on maternity leave, and employees with certain medical conditions) as eligible to work from home. Any work-at-home arrangement should:

- Be in writing.
- Identify the time period the work-at-home will be allowed.
- Identify the government equipment and supplies needed by the employee at home and how the Laboratory and employees will transfer and account for the equipment and supplies.
- Identify if telecommuting will be needed and allowed. If telecommuting is authorized, a VPN (Virtual Private Network) account will need to be obtained from the IS Office.
- Be reviewed by the Ames Laboratory Human Resources Office prior to commencement.

Foreign National Access
In order for foreign nationals to be granted access, the Foreign Visits and Assignments Form (Form AL-473 located here: https://www.ameslab.gov/directors-office/documents/form/foreign-visits-and-assignments-form) must be completed and approved by the Program Director and the Chief Operations Officer. A standard security plan encompasses all foreign nationals accessing the low enclave data.

If the foreign national is an Ames Laboratory employee or associate from a terrorist country or accessing moderate data, an individual security plan is developed. The Foreign National Access to Cyber Systems Form (https://www.ameslab.gov/is/documents/form/foreign-national-access-cyber-systems) is completed to indicate the computer systems that will be accessed while employed or associated with the Laboratory. The form contains:

- A description of the computing resources the foreign national will use.
- The location of the resource(s) and the purpose for use.
- The host must indicate if the foreign national will be accessing a system containing sensitive information and if the individual will need remote access.

5.5 Audit & Accountability

System Monitoring

All system and network data on the Ames Laboratory network is subject to monitoring at any time, as indicated in the DOE warning banner and site policy. Users should not use Ames Laboratory resources for any activity or information which they would not want reviewed or made available to Ames Laboratory management staff.

Program & Department Monitoring: Cyber Security Walk-Through Program

A walk-through is a planned tour of a department/program on a routine basis used to assess the cyber security implementation in accordance with Ames Laboratory policy. This activity also fulfills the sensitive system and management cyber security training requirements.

The department manager or program director and the ACSM are notified two weeks prior to the scheduled walk-through and given the general scope and a brief description of the walk-through process. During the evaluation, the walk-through team observes and evaluates the area, testing systems for technical controls and reviewing operational and management controls with system administrators.

The assessment is included in a final report and issues are assigned severity ratings based on consequence and risk potential. The cyber security team and department/program officials review the report and discuss appropriate corrective actions. The program or department is responsible for performing any corrective actions.

Email Monitoring

Cyber security staff monitor the email system to ensure that our computing resources are properly protected and operating effectively. However, staff email messages and other user files are not examined unless such examination is:

- Authorized by appropriate management.
- Performed to ensure adequate network service is being provided.
- Required as part of an audit or an investigation.

Although email system monitoring is performed only under the above circumstances, staff should never assume that their email cannot be read or accessed by anyone else. Because email sends data across the network, it is also subject to network monitoring. If Ames Laboratory staff discovers anything indicating misconduct, the information contained in email messages or other communications may be used to document such conduct. These may be revealed to the appropriate authorities, both internal and external to Ames Laboratory.

For email that is sensitive or confidential in nature, an encryption package such as Pretty Good Privacy (PGP) or Entrust should be used. Contact the IS Office for more information about email encryption.

The addresses of all mail sent or received by the mail server is logged. All undeliverable messages are returned to the sender, sent to postmaster@ameslab.gov, and reviewed by members of the system administration staff. Logging email activity ensures that no email is lost due to configuration problems and that problems with mail delivery can be diagnosed.

Network Monitoring

All network data is captured and stored for approximately two weeks by cyber security monitoring equipment. This data is reviewed by automated processes which monitor for signs of malicious network activity. Suspected malicious traffic is then manually reviewed to make a determination about the nature of the attack and the risk to computing resources.

Network connection logs are captured centrally and stored for a period of at least one year. This includes data such as which hosts connected to which other hosts, what services were used, and how much data was exchanged. This information is reviewed as necessary to correlate network activity with other activity alerts.

Intrusion detection systems generate alerts and additional logging data for anomalous network events. Some of these include:

- Attempted access to systems which do not exist on the network.
- Attempted network access to many systems or network access to many ports on a system in a short period of time.
- Detection of suspicious protocols on non-standard ports, such as IRC or peer to peer traffic.

System Monitoring

System baseline guides include settings to ensure that crucial security information is logged. This information is used to aid investigators in the event of unexpected system problems or potential intrusions. For systems not covered under a baseline guide, the following audit events should be recorded where possible:

- Successful and failed login attempts.
- System warning and error messages.
- A record of mail sent from the system.
- Startup and shutdown status messages.

5.6 Configuration Management

Configuration management is the process of tracking changes to the system, which ensures that the changes are reflected in documentation and do not unintentionally or unknowingly diminish security. A log book can be purchased from the storeroom to track configuration changes and provide important documentation for system users. Automated central processes are also in place to track patch and configuration status of systems on the Ames Laboratory network.

Patch Management

An important component of configuration management is patch management. Complex operating systems and applications have security holes, and to ensure the security of all users on the network, Ames Laboratory uses centralized patch management software and procedures. All systems on the Ames Laboratory network are required to follow these procedures or to submit a Baseline Guidelines Exception Form (Form 48400.025). The form is available here: https://www.ameslab.gov/is/documents/form/baseline-exception.

The following products are employed to meet the requirements of a full patch-management solution at Ames Laboratory:

- **Windows Server Update Services (WSUS)** is available from Microsoft at no charge. It provides patch management for Windows operating systems and some Microsoft software products, such as Office. Only compatible Windows versions can use this product, including Windows 2000, Windows Server 2000, and Windows Server 2003. Systems not supported by this product must be isolated in the Legacy VLAN network segment, and will have network access restricted.
- **Nessus** is an open source vulnerability scanner used to scan systems on the Ames Laboratory network. This product scans all systems daily for common vulnerabilities, many of which can be fixed by applying current patches. This, coupled with the Spacewalk Software below, provides minimal patch management for Linux and Mac Systems.

Contact the IS Office for more information on this subject.

Inventory Management

Inventory management is required by DOE to determine exactly what systems, software, and network devices exist on their network. In addition, inventory information is critical to improving the accuracy of vulnerability scans, risk analysis, and the timely dissemination of applicable security information. Ames Laboratory uses several systems to provide inventory information on general systems.

- **Netreg**: All systems with an IP address beginning with ‘147.155’ are required to register via the Netreg database system prior to connecting. Registration includes collecting information on the operating system, hardware class, and tracking. Group Administrators and ACSMs should manually update the Netreg system whenever system hardware, operating system, or ownership changes. For more details, contact the IS Office.
- **Property Management**: The property management system and database track all computer purchases through Ames Laboratory using a property number. Periodically these items must be re-inventoried to ensure that they are still on site. This property number is also used in the Netreg system to allow physical identification of a particular computer.
- **Microsoft System Management Server**: This system collects automated information on installed software and hardware on Windows systems in the Active Directory domain.
- **Spacewalk Software**: An open-source management solution for Linux systems. This can be used to determine the version of software installed on these systems and if they are up-to-date.

In addition, some systems require more rigorous monitoring. Sensitive, internet accessible, and central server systems are also required to run OSSEC or Samhain Host Intrusion Detection Systems (HIDS). These two open source products provide file-level change monitoring to detect modified files.

Best Practices

All Ames Laboratory system administrators, including administrators of systems storing sensitive information, should follow these procedures to ensure a secure system:

- Patch operating system and applications on a daily basis.*
- Update anti-virus software daily.*
- Implement a host-based firewall such as Windows Firewall, or iptables.
- Review operating system, application, firewall, and HIDS log files on a daily basis and research (on the internet or by contacting the IS Office) any unfamiliar messages.

*Note: These procedures can be configured to run automatically, but should be manually checked weekly.

5.7 Contingency Planning

Contingency Plans

Contingency plans describe procedures currently in place and the resources (e.g., backup tapes, personnel) required to respond to abnormal situations. Contingency plans ensure that computer application owners can resume Ames Laboratory research and business as efficiently as possible following a disaster or other severe computing interruption.

All system administrators should plan for contingencies to enable the speedy recovery of data and to minimize the negative impact on Ames Laboratory systems in the event of misfortune such as a malicious attack, hardware failure or destruction, software crashes, or unintentional misuse. Each program/office should have a written contingency plan covering its major computing assets. A solid contingency plan covers the data path from acquisition to analysis and will include a system backup, a system recovery checklist or guide, and a log of changes made to the system (e.g., installed applications, important configuration changes, and anything that would need to be redone to recover the computing resource).

The disaster recovery template for a program/office is located here:
https://www.ameslab.gov/operations/faq/there-template-creating-disaster-recovery-plan

Data Backup and Storage

Performing regular system backups is critical to data security as it minimizes the loss of data and software caused by accidental deletion or a major disaster (e.g., fire). Choose a backup procedure (mode, frequency, number of copies, and media storage site) that matches the importance of the data. Backups of application and system files should also be made, though such backups may consist of installation media copies.

Backups should be stored securely and tested for usability. It is important to document what data is backed up and what data is considered expendable. This documentation will provide crucial information for system users to ensure no data is lost due to conflicting expectations.

5.8 Identification & Authorization

Least Privilege

Least privilege is defined as granting users only the access they need to perform their official duties efficiently, effectively, and securely. For example, it is possible to grant system administrator privileges to all users of the Local Area Network (LAN), allowing every user to change the system configuration whenever he or she wanted. In reality, these unnecessary privileges lead to unnecessary risks and exposure to cyber attacks. Therefore, only users with training in system administration are granted system administrator privileges, and the other users are granted only those privileges necessary in order to accomplish their work.

ACSMs, group administrators, and IS staff have separate central accounts named *adm-<username>* for performing administrative tasks. These accounts must be maintained separately and should not be used for normal day-to-day activity. Computers in the active directory domain will allow these accounts to perform administrative functions automatically.

Separation of Duties

Separation of duties is the division of roles and responsibilities so that a single individual cannot weaken a critical process. For example, the person who enters payee information into a system should not be the same person who authorizes payments to be made or has the ability to delete a payee from a system. This separation of entry, approval, and deletion duties helps ensure that a financial system is not exploited to make and cover up improper payments. This separation of duties should also apply to approving, implementing, and auditing computer accounts. New accounts are requested and provided by the IS office, with approval provided by the program director and group leader, and the ACSM or group administrator.

5.9 Incident Response

Cyber Security Incidents

The DOE Cyber Security Incident Management Manual (DOE M 205.1-8) is used to categorize cyber security incidents according to potential negative impact to information and/or information systems. A “security incident” is an adverse event that threatens the security of information resources. This DOE manual defines two types of cyber security incidents:

Type 1

Successful incidents that potentially create serious breaches of Ames Laboratory cyber security or have the potential to generate high-visibility media interest.

- **Compromise/intrusion**: System compromise or intrusion by unauthorized persons.
- **Website defacement**: Damage to a web site’s appearance and integrity.
- **Malicious code**: Persistent attempts or successful infection by malicious code (e.g., viruses, Trojan horses, or worms)
- **Denial of service**: Intentional or unintentional denial of service (successful or persistent

attempts) that affects or threatens critical service or denies access to all or one or more large portions of a network.

- **Critical infrastructure protection (CIP):** Any activity that adversely affects an asset identified as critical infrastructure.

- **Unauthorized use**: Any activity that negatively affects an information system's normal, baseline performance and/or is not recognized as being related to Ames Laboratory's mission.

Type 2

Attempted incidents that pose potential long-term threats to Ames Laboratory cyber security interests or that potentially degrade the overall effectiveness of the Lab's cyber security posture.

- **Attempted intrusion**: An exploit that stands out above the daily noise level and would result in unauthorized access (compromise) if the system were not protected.

- **Reconnaissance activity**: Persistent surveillance probes and scans that stand out above the daily noise level and may be designed to collect information about network vulnerabilities.

- **Unauthorized use**: Computer usage for anything but its intended purpose - information is obtained without permission or the system is used to gain access to DOE data without proper permissions.

Common Incident Symptoms

Some common symptoms of a computer system under attack include:

- Unexplained discovery of new files or unfamiliar filenames, or changed file dates or sizes.
- Multiple unexplained logon attempts or successful logins, or your account locked.
- Unauthorized creation of new user accounts.
- Missing or unusually full system logs.
- Activation of a system alarm or similar indication of an intrusion.
- System crashes.
- Unauthorized processes running.

5.10 Incident Response

When signs of a cyber incident are detected, call the IS Help Desk at 294-8348 for assistance and provide your name, office location, symptoms experienced, and computer system's IP address (similar to 147.155.xxx.xxx). Leave the system as is unless otherwise directed by a member of the Incident Response Team (see this url https://www.ameslab.gov/operations/faq/please-identify-cyber-security-staff-ames-laboratory for a list of Cyber Security and Incident Response staff).

If a cyber security incident has occurred, the hard disks from the affected system will need to be retained by IS as evidence in the event of prosecution. The system will need to be restored from backup or reinstalled prior to accessing the network again.

For more information, review the Incident Response Team training document (https://www.ameslab.gov/is/documents/plan/cyber-incident-response-plan).

Social Engineering

Social engineering is an attacker's manipulation of the natural human tendency to trust. The goal is to obtain information that will allow unauthorized access to a system and the information that resides on it. Several high-profile compromises in DOE and other government agencies have been the result of social engineering attacks. Attack examples include convincing users to:

- Open an email attachment.
- Run a program from a website.
- Load a CD-ROM or USB drive.
- Give out their passwords over the phone, via email, or through a fake website.

Social engineering is often an easier way for attackers to gain illicit access to systems than traditional technical exploits. Even for very technical people, it's often much simpler to pick up the phone and ask someone for their password.

To protect against social engineering attacks, use the following best practices:

- When using usernames and passwords in open public places, be aware of others, especially those standing where they have a view of your keystrokes (shoulder surfing).
- Never give a password over the phone or email!
- Never click on web links in an email; copy and paste the URL into a browser instead.
- If an unexpected CD, DVD, or other media is received, verify the source prior to loading it into a computer.
- Never insert unknown USB drives or other rewritable media into your computer; bring them to the IS Office to verify that they are clean first.
- When an urgent threat notice is sent about a current e-mail phishing attack, ensure that all users in the area are aware of the threat. Pay special attention to users who may have been out of the office and missed any announcements; be sure to speak with them before they check their e-mail.
- Phishing attacks and other forms of social engineering are also cyber attacks. Unexpected e-mails or phone calls, unsolicited CVs, resumes, or requests for information should all be reported to abuse@ameslab.gov.

JC3 Notices

Alerts and security warnings from JC3 are distributed to ACSMs for review. If security issues are identified for a specific system configuration under an ACSM's control, mitigation of the security issue is necessary. The mitigation process can be a configuration change or the installation of available operating system/application patches.

5.11 Media Protection

Cleaning and Sanitization of Hard Drives

All DOE-owned or managed hard disks, tapes, or CDs must be physically destroyed upon excess. In addition, any licensed software (other than the operating system and software covered under the Microsoft Campus Agreement (MCA)) should be removed from the system prior to excess unless the licensed software is being transferred with the computer to a specific user. See http://it.iastate.edu/mca/ for a list of software covered under the MCA.

To facilitate this process, any computing equipment scheduled for excess will first be delivered to the IS office for sanitization. The hard disks will be removed and destroyed. Once the system has been sanitized, it will be tagged for the warehouse where it will enter the equipment pool.

Systems not processed through the Ames Laboratory Excess system (i.e., systems not going out to the warehouse but are being transferred elsewhere) must be sanitized. The recommended procedure for sanitizing computer hard drives is to use Darik's Boot and Nuke (http://www.dban.org/) with the American DoD Standard Wipe option. A minimum of three-pass overwrites is required for sanitizing unclassified computer media.

5.12 Physical & Environmental Protection

Best Practices

Take the following steps as appropriate to help keep your data secure:

- Use a screen saver password and network passwords.
- Close and lock your office door when you leave a system unattended for extended periods of time.
- Know the people who have routine access to your area and challenge people in your area who do not have routine access.
- Immediately report any missing equipment or data (even suspected data loss or compromise) to Environmental Safety, Health, & Assurance, your ACSM, or the CSM.
- Take extra care with hardware that can be easily stolen such as PDAs and laptops.
- Use some form of encryption on portable systems and media for private data.

5.13 System & Services Acquisition

Copyright Licenses

Allowing others to illegally copy or use copyright material (e.g., music or software) makes a user subject to laws such as the No Electronic Theft Law (NET Act) (http://www.justice.gov/archive/opa/pr/1999/August/371crm.htm) and the Digital Millennium Copyright (DMCA) Act (http://www.copyright.gov/legislation/dmca.pdf). Network activity is logged and reviewed to monitor the usage of copyright licenses.

Software License Restrictions Issues

Proof of license for all software products used on your assigned system(s) must be maintained. Proof of license includes possession of the original vendor distribution media, vendor-distributed manuals, and/or a vendor receipt or acknowledgment containing the license number.

Federal Copyright Law governs the use of computer software except where authorized by the licensing agreement of particular software. It is illegal to make or use illegitimate copies of software. Ignorance is no excuse under the Copyright Protection Act. Violation of licensing agreements is punishable by fines and/or imprisonment.

It is Ames Laboratory's policy to adhere to all copyright agreements of software owned by or used by Ames Laboratory personnel. **No Ames Laboratory employee will knowingly violate the license agreement of the software she or he is using.** It is the responsibility of each computer user to follow the licensing agreement of all software that is being used and to keep documentation, sales receipts, original diskettes, purchase orders, registration certificates, etc., proving the software was purchased legally.

The Microsoft Campus Agreement (MCA)

Software licensed from Ames Laboratory or Iowa State University under the Microsoft Campus Agreement (MCA) can be used without additional proof of license. ISU faculty and staff are eligible to participate in the Microsfot Home Use Program (HUP). The software may be used at home for personal use. More information is available here: https://www.it.iastate.edu/services/software/hup/

Other Site-Licensed Software

Software site-licensed by Ames Laboratory or Iowa State University does not require possession of media, manuals, and/or physical license. Software available via the Iowa State Scout utility or from http://www.sitelicensed.iastate.edu can be used on computers at home at no additional charge. You will need to use your ISU logon to access the information on this site. Information on ISU software available for download is available here: https://www.it.iastate.edu/services/software. Ames Laboratory or Iowa State University purchased software can be used for personal use at home, provided that the software license permits secondary use.

Computing Resource Usage

While DOE systems are available for limited personal use, the use of computer resources for the following activities is **not** permitted:

- Accessing pornographic web sights and material.
- Developing applications or conducting commercial activities for personal gain.
- Illegally downloading copyrighted material.
- Accessing offensive or questionable material.
- Performing personal activities that may cause congestion, delays, or disruptions of service to others.
- Computer gaming on Ames Laboratory computer systems.

Periodic Waste, Fraud, and Abuse reviews on all Ames Laboratory computers and network resources can be conducted by the ACSM, as directed by the Program Director, Department Manager, or IS Office staff to ensure that software and the usage of the computer comply with

Laboratory policies. Any unauthorized files found may be purged and the misuse reported to the employee's supervisor, ACSM, and CSM.

Peer-to-Peer (P2P) is an example of software that is considered inappropriate on the Ames Laboratory network unless prior approval is obtained. Examples of unauthorized P2P software are Kazaa, Bearshare, and Emule/Edonkey. There are legitimate uses for P2P software, however prior to using software for this purpose, the IS office must be notified.

5.14 System & Communication

Encryption

Encryption is the encoding of information so that only specific individuals can decode it. As a data security measure, encryption is a very effective way of protecting information from unauthorized access when stored on media (e.g., CDs and disks) or when transferred over digital communication lines (e.g., via email or the Internet). In addition to keeping data private, encryption can be used to verify that the information received is the same information that was sent (data integrity) and that the information did not come from a malicious entity masquerading as a known source (data authenticity).

For file system encryption, the Mac OSX FileVault, Windows BitLocker, or a variety of Linux encryption mechanisms can be used. The use of file system encryption is highly encouraged on laptops and other portable devices and for any information that should be kept private. This encryption will protect data confidentiality in the event of hardware theft or unauthorized access as another user. It will **not** protect against compromised passwords, malware, or data loss.

Email encryption and verification can be accomplished through several mechanisms. DOE provides Entrust, a certificate-based email encryption package, free of charge. The use of Pretty Good Privacy (PGP), or certificate-based X.509 encryption is also acceptable. If you want to use a different encryption package or need help getting set up with encryption, please contact the IS Office.

While data encryption is an excellent means of protecting information, it can also put Ames Laboratory at risk because of the potential for the information to become inaccessible if the encryption key is lost or misplaced (e.g., you can't access the information that you need because you don't have the ability to decrypt it). While encryption passwords should be long and complex enough to be secure, they must also be memorable! A good method of choosing such a password is to think of a meaningful sentence
or phrase and use the first letter from each word.

When encryption is used to protected sensitive data, DOE requires that FIPS140-2 compliant software and hardware are used. For a complete list see:
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

5.15 System & Information Integrity

Spam

Spam is unsolicited junk email (and sometimes unsolicited junk newsgroup postings from outside the Ames Laboratory). It is recommended that you immediately delete any spam you receive rather than respond to it, even if it claims to allow a mechanism to un-subscribe. Ames Laboratory has instituted some general spam filters centrally, and the use of client-based spam filtering such as the Junk filters in Eudora and Thunderbird is highly encouraged.

Unknown Email and Attachments

Email has become one of the most common vectors by which systems are compromised. Often these attacks come in the form of malicious attachments or web pages that the user is convinced to open or visit. Some safe practices that can help prevent email-based compromises include:

- Before opening any unexpected email attachments, check with the sender to ensure its validity. Often
  a quick email or phone call can save hours in incident response and system reconstruction time.

- If opening an attachment from an unknown source cannot be avoided, use this procedure:

    1. Ensure that you are logged in as a non-administrator.
    2. Save the file to your hard disk.
    3. Scan the file using your antivirus software.
    4. Open the file.

Tips and Guidelines

- The “From:” address in an email is easily forged. Never trust this as the only verification that a message is really from that source.

- Be careful when forwarding email messages. Use common sense: if you would not forward a paper copy of a memo with the same information, do not forward the message.

- Be careful what you write. Email is not the same as conversation. It is a written record and can be duplicated freely. Email messages sent to customers or third-party suppliers may be construed as legally-binding. Do not write or keep anything that you would not send in a formal letter or mention in conversation.

- When replying to a message, make sure you know who will receive your reply. Often, Reply All is not only unnecessary but also results in a large number of people receiving numerous messages that are irrelevant to them and disruptive to their work. This is especially true when distribution lists are used.

- When sending a message to a distribution list, use the blind copy (BCC) feature to address the list. This prevents everyone receiving messages when a recipient uses Reply All.

- Scan all attached software and files for viruses before opening them.

Malware

Malware is a class of computer programs that perform unauthorized actions on a computing system without the user’s knowledge. Ames Laboratory has effective means of protection against the several forms of malware. One of the most important overall protections is the use of non-administrative accounts on systems for day to day work. This prevents malware from running as an administrator and limits potential damage.

Viruses and Worms

A computer virus attaches to a computer system and spreads to other programs and linked systems. A virus may also write a message on a computer screen, send email on behalf of the user, or destroy files accessible by the user. Viruses are introduced to a computer by many methods, including:

- downloading files from the Internet,
- peer-to-peer file sharing,
- opening e-mail attachments,
- using rewriteable media (e.g., floppy disks, zip disks) of unknown or questionable origin,
- copying files or executing programs from a network.

Check any shareware and freeware products for viruses before they are installed on an Ames Laboratory computer system. One of the most common means of infecting Ames Laboratory systems is transferring files from home systems to Ames Laboratory systems.

A worm is very similar to a virus, but it is self-contained and doesn't have to attach to another program to cause damage. However, it still must be copied to a system in some fashion, commonly through email attachments or Windows file shares.

Ames Laboratory has site-licensed virus-protection software for all Windows (McAfee) and Macintosh (Virex) systems, which includes worm protection. The open-source product ClamAV provides protection for Linux systems. McAfee and Virex software is available via the Iowa State Scout utility or the Iowa State web site for users with an Iowa State Net-ID (https://www.sitelicensed.iastate.edu).

Antivirus software should be configured with auto-protect enabled and scheduled to perform a full system scan and automatic update at least weekly on all appropriate Ames Laboratory systems. You are also encouraged to install the site-licensed software on personally-owned systems.

Instructions on installing and configuring McAfee and Virex are covered in the Baseline Configuration Guide for Win2k and Window desktops (https://wiki.internal.ameslab.gov/wiki/Baseline_Guides).

Spyware

Spyware software is commonly installed as part of ad-supported freeware and shareware applications or from unexpected software installed by malicious web sites. They invade users' privacy and compromise data confidentiality by tracking personal information (e.g., browser history file, favorites lists, temporary Internet files, and cookie files), open unwanted pop-up windows, modify browser settings, and even record passwords or grab files.

The IS Office recommends installing Microsoft Windows Defender software and running it on a daily basis to detect and remove spyware from your computer. Defender can be configured to update and scan on-access. Instructions on installing Defender are covered in the Baseline Configuration Guide for Windows (https://wiki.internal.ameslab.gov/wiki/Baseline_Guides).

Hoaxes

Some virus announcements are actually hoaxes. If you receive an email message about a virus from anyone other than the IS Office or your ACSM., forward the message to the IS Office to verify if it is a virus or a hoax. Do not forward the message to anyone else.

6.0 ADDITIONAL INFORMATION

References

Confidence and familiarity with a computer system increases with practice and experience. The better the system and software are understood, the more effectively the system and information can be managed. Please refer to the following references for more information.

- Specific information on Ames Laboratory and DOE Cyber Security can be found here: https://wiki.internal.ameslab.gov/wiki/Cyber_Policies_and_Procedures

- Specific information on Iowa State University Cyber Security can be found here: http://www.it.iastate.edu/policies/

- Specific Ames Laboratory training classes are available. The list of courses is located here: https://www.ameslab.gov/is/documents/cstraining

- Training for general-use computer systems is also available at Iowa State University. You can also contact the Iowa State University Information Technology Services for information about current topics and training schedules at http://www.it.iastate.edu/training/

- NIST security recommendations: http://csrc.nist.gov/publications/PubsSPs.html

- DOE Office of the CIO Security Implementation Guidance: http://energy.gov/cio/policy-and-guidance